

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 02-301241
 (43)Date of publication of application : 13.12.1990

(51)Int.CI.

H04L 9/06
 G06F 13/00
 G09C 1/00
 H04L 9/14

(21)Application number : 01-121861

(71)Applicant : NIPPON TELEGR & TELEPH CORP
 <NTT>

(22)Date of filing : 15.05.1989

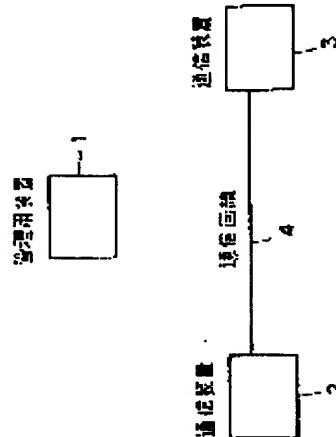
(72)Inventor : KOBAYASHI TETSUJI

(54) DELIVERY SYSTEM FOR COMMON KEY

(57)Abstract:

PURPOSE: To eliminate the need for an open public table and to sufficiently protect the secrecy of a communication equipment by providing a power cryptographic equipment to each communication equipment and using the power cryptographic equipment.

CONSTITUTION: A management equipment 1 gives public information in common to the communication system and secret information generated corresponding to the public identification information of the communication equipment 1 to each communication equipment and each communication equipment stores the public information and the secret information. When the power cryptographic equipment is used to deliver the common key, the public information in common to the communication system and the secrecy information for each communication equipment are used for the text to be sent and a communication equipment 2 gives a digital signature to apply the transmission to the communication equipment 3. The communication equipment 3 confirms the adequacy of the received digital signature, adds the digital signature of the communication equipment 3 to other text relating to the delivery of the common key, sends the result to the communication equipment 2, and the communication equipment 2 confirms the adequacy of the digital signature to confirm the adequacy of the communication equipment 3. Since the management equipment cannot recognize the common key, the secrecy of the common key of the communication equipment is maintained.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

④日本国特許庁 (JP) ⑪特許出願公開
②公開特許公報 (A) 平2-301241

⑤Int.Cl.
H 04 L 9/06
G 06 F 13/00
G 09 C 1/00
H 04 L 9/14

識別記号 351 E

厅内整理番号 7459-5B
7343-5B

⑥公開 平成2年(1990)12月13日

6945-5K H 04 L 9/02
審査請求 未請求 請求項の数 1 (全12頁)

⑦発明の名称 共通鍵の配送方式

⑧特 願 平1-121861
⑨出 願 平1(1989)5月15日

⑩発明者 小林 哲二 東京都千代田区内幸町1丁目1番6号 日本電信電話株式会社内
⑪出願人 日本電信電話株式会社 東京都千代田区内幸町1丁目1番6号
⑫代理人 弁理士 草野 卓

明細書

1.発明の名称

共通鍵の配送方式

2.特許請求の範囲

(1) 一つ以上の管理用装置と、二つ以上の通信装置により構成される通信システムにおいて、一つの管理用装置が、通信システムで共通な公開情報および通信装置の識別用の公開識別情報を用いて生成した秘密情報を、各通信装置に付与し、各通信装置は、通信システムで共通な公開情報および通信装置ごとの秘密情報を保持する第1の過程、および、

二つ以上の通信装置が、ベキ乗暗号装置を用いて共通鍵の配送を行うときに、送るべき電文の1つに対し、上記通信システムで共通な公開情報および通信装置ごとの秘密情報を用いて、各通信装置がディジタル署名を付与することにより、互いに相手側通信装置から受信した電文の正当性確認を行う第2の過程、を有することを特徴とする共通鍵の配送方式。

3.発明の詳細な説明

「産業上の利用分野」

この発明は、通信回線により通信を行う二つ以上の通信装置の間で、共有する暗号鍵（即ち、共通鍵）をベキ乗暗号装置を用いて配送する共通鍵の配送方式に関するものである。なおここで通信装置は、通信機能を有する装置、すなわち、電子計算機、端末装置、電子交換機、通信制御装置、通信処理装置、またはICカード、などを表すとする。

「従来の技術」

通信装置の間で秘密情報を安全に行うためには、暗号を用いる通信が有効である。暗号法には慣用暗号と公開鍵暗号があることが知られている。慣用暗号では暗号鍵の配送が必要である。暗号鍵には、暗号化用の鍵である暗号化鍵と、復号化用の鍵である復号化鍵がある。慣用暗号は、暗号化鍵と復号化鍵が同一な暗号法を意味する。二つ以上の通信装置で共有する暗号鍵を、共通鍵と呼ぶ。慣用暗号の暗号アルゴリズムには、例え

特開平2-301241(2)

ば、DES暗号（"Data Encryption Standard"、*Federal Information Processing Standards Publication 46*、U.S.A.、(1977年)）、及びFEAL-8暗号（宮口ほか著：“FEAL-8暗号アルゴリズム”、研究実用化報告、第37巻第4／5号、(1988年)）などがある。公開鍵暗号のアルゴリズムには、例えば、RSA暗号（"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"、*Communications of the ACM*、Vol. 21、No.2、pp.120-126、(1978年)）、Rabin暗号（"M.Rabin著：Digitalized Signatures and Public-Key Cryptosystems"、*MIT/LCS/TR-212, Technical Report*、MIT(1979年)）などがある。

複数の通信装置では、公開鍵系の手法により、事前に秘密情報を共有することなく通信メッセージ（声、電文）に、ベキ乗暗号装置を用いて共通鍵の配達または生成を行う方式が既に知られている。その第1に、二重暗号を用いる方式（例えば、「小林哲二著：“暗号通信における2重暗号

型鍵配達方式”、電子情報通信学会論文誌、Vol. J71-D、No.9、pp.1815-1822、(1988年)」における基本処理手順を参照）である。第2に、Diffie-Hellmanによる共通鍵配達方式（例えば、“New Directions in Cryptography”、*IEEE Trans. on Information Theory*、IT-22、pp. 644-654 (1976年) を参照）である。第3に、公開鍵暗号（例えば、RSA暗号、Rabin暗号）などである。公開鍵系の手法を用いた共通鍵配達では、公開された情報の安全性を保護するために、公開鍵の管理を行う必要があるのが欠点である。このための対策として、通信システム内で通信装置を一意に識別できる公開識別情報（声、通信システム内で一意に付与された公開の識別情報であり、例えば、電話番号、住所、通信装置識別子、など）を用いる方式がある。ディジタル署名は、メッセージの作成者とメッセージ内容の正当性を保証する機能である。公開識別情報に基づくディジタル署名の安全な方式として、Fiat-Shamirによる方式（A.Fiat and A.Shamir著：“How To Prove

Yourself : Practical Solutions to Identification and Signature Problems”、*Proceedings of CRYPTO 86*、Springer-Verlag、Lecture Notes in Computer Science 263、pp.186-194(1987年)）が提案されているが、その方法では共通鍵の配達はできない。

「発明が解決しようとする課題」

従来に提案されている公開識別情報を用いる共通鍵配達方式では、管理用装置が通信装置の共通鍵を知ることができること等の秘密保護に問題がある。この発明の目的は、複数の通信装置間における共通鍵の配達において、公開鍵を不要とし、かつ通信装置の秘密保護が十分な共通鍵の配達方式を提供することである。

「課題を解決するための手段」

この発明は、一つ以上の管理用装置と、複数の通信装置により構成される通信システムに適用する。各通信装置は、通信システム内で一意に定まる公開識別情報を有することとする。各通信装置は、ベキ乗暗号装置を備えている。ベキ乗暗号装置

を用いることにより、複数の通信装置の間では、事前に秘密情報を共有することなく共通鍵の配達を行うことができる。通信装置の間の共通鍵の配達は、次の二つの独立な過程により実現する。

①共通鍵配達の第1の過程：

各通信装置が管理用装置に登録する時に、管理用装置は、通信システムで共通な公開情報と、通信装置の公開識別情報を対応して生成した秘密情報を、各通信装置に付与し、各通信装置はそれらの公開情報と秘密情報を保持する。なお、管理用装置は、個々の通信装置に対応して生成した秘密情報を、通信装置に付与した後では、保持する必要はない。

②共通鍵配達の第2の過程：

管理用装置からそれぞれ秘密情報を保持している複数の通信装置（例えば、通信装置aと通信装置b）が、共通鍵の配達を行うときに、通信装置aは、共通鍵の配達に用いた電文に、ディジタル署名を付加し、通信装置bに送信する。通信装置bは受信したディジタル署名の正当性を確認

する。更に、通信装置 α は、共通鍵の配信に関した別の電文に、通信装置 α のディジタル署名を付加し、通信装置 α に送信する。通信装置 α は、ディジタル署名の正当性を確認することにより、通信装置 α の正当性を確認することにより、通信装置 α の正当性を確認する。また、これらの電文から、各通信装置は共通鍵を共有する。ここで、電文の数、電文内容、およびディジタル署名の対象とするデータは、共通鍵を配信する方式により、異なっている。この共通鍵を配信する方式としては従来より知られているベキ乗暗号装置を用いる各種の共通鍵配信方式を利用できる。

「作用」

前述の手段において、通信装置の間で共有する共通鍵の値は、管理用装置では生成できないので、管理用装置は、共通鍵を知ることができないため、通信装置の共通鍵の秘密が保たれている。また、公開鍵は不要である。

「実施例」

第1図は、この発明が適用される通信システムの一構成例であり、管理用装置1、通信装置2、

ると、

$$C = \exp(M, K) \bmod p$$

$$M = \exp(C, K) \bmod p$$

となる。ここで、 $0 \leq M < p$ 、 $0 \leq C < p$ 、かつ

$$K \cdot K^{-1} \equiv 1 \pmod{p}$$

である。 $\phi(\cdot)$ は、オイラーの関数である。即ち、 p の素因数を、 P, Q, R, \dots とすると、

$$p = P^{\alpha} Q^{\beta} R^{\gamma} \dots$$

であるから、

$$\phi(p) = p(1-1/P)(1-1/Q)(1-1/R) \dots$$

である。したがって、 p が素数のときは、

$$\phi(p) = p - 1$$

である。ベキ乗暗号装置は、ハードウェア、又はハードウェアとソフトウェアの組み合わせにより実現できる。ベキ乗暗号装置における、ベキ乗剰余、および逆数の計算法などには、任意の方法を利用できる。それらの計算法は、例えば、「池野ほか著『現代暗号理論』、電子情報通信学会、(1986年)」などに述べられている。

第2図は、ベキ乗暗号装置11の一構成例である

通信装置3、通信回線4で構成されている。通信装置が、二つ以上ある場合も同様である。次に、記法を述べる。整数は、この発明の実施例では、負でない整数を意味する。A、B、t及びNを任意の整数とするとき、BについてのNを法とする剰余がAであることを、 $A \equiv B \pmod{N}$ と表す。AとBがNを法として合同であることを、 $A \equiv B \pmod{N}$ と表す。Aのt乗の法をNとする剰余である、 $A^t \pmod{N}$ を、 $\exp(A, t) \pmod{N}$ と表す。Iは、二つ以上のデータのそのままの値の連結を表す。⊕は拡張的論理和の演算を表す。

通信装置 α の公開識別情報を、ID α とする。ここで、wは任意の値であり、例えば、通信装置 α の識別子はID α 、通信装置 α の識別子はID α となる。公開識別情報は、通信システム内では、一意に定まるとする。

次に、ベキ乗暗号装置について述べる。各通信装置は、ベキ乗暗号装置を備えるものとする。整数のパラメータを、平文をM、暗号文をC、暗号化鍵をK、復号化鍵をK⁻¹、公開の整数をpとす

る。信号路12は、ベキ乗暗号装置11へ入力データを入力するための信号路であり、任意の整数のデータMを入力する。信号路13は鍵（暗号化鍵または復号化鍵）の入力のための信号路であり、暗号化鍵Kを入力する例を示してある。信号路14は法の値pの入力のための信号路である。ベキ乗暗号装置11は、入力データMについて、暗号化鍵Kの値を指數とするベキ乗の法の値pによる剰余を計算して、信号路15から出力データCを出力する。ここで、 $C = \exp(M, K) \pmod{p}$ である。

ベキ乗暗号装置16は、ベキ乗暗号装置11と同じ装置であり、復号化鍵K⁻¹を鍵として入力している例である。信号路17から入力された暗号文Cは、ベキ乗暗号装置16により変換されて、信号路20から平文Mを出力する。

第3図は、ベキ乗暗号装置21の一構成例である。ベキ乗暗号装置21は、ベキ乗暗号装置11、16とは異なる型のベキ乗暗号装置である。この型のベキ乗暗号装置では、整数のパラメータを、

H, t, p とすると、

$$J = \exp(H, t) \bmod p$$

となる。ここで、 $0 < J < p$, $0 < H < p$, かつ $0 \leq t < p$ である。即ち、信号路 23 からは、整数 H を入力する。信号路 24 からは、法の値 p を入力する。信号路 22 からデータ t を入力して、データ H および法の値 p を用いて、信号路 25 から、出力データ J を出力する。

次に、管理用装置と通信装置で使用する関数 $f(\cdot)$ について述べる。関数 $f(\cdot)$ は、任意の数値 θ を、

$$0 \leq f(\theta) < n$$

の値に変換する関数であり、 $f(\theta)$ から θ を求めるのは、計算時間から見て困難であるとする。 $f(\cdot)$ は、例えば、次のようにして実現できる。 θ は、長さが n 未満のときは、必要により、0 を後に付加して、 θ の長さが n になるようにし、かつ個々の $\theta_i < (i = 1, 2, \dots, m)$ は暗号装置のブロック長になるように選択して、

$$\theta = \theta_1 \parallel \theta_2 \parallel \dots \parallel \theta_m$$

まず、管理用装置は、各通信装置が管理用装置に登録を行うときに、次の共通鍵配送の第1の過程を実行する。

共通鍵配送の第1の過程：

ステップ 1：

管理用装置は、管理用装置の秘密情報として、素数 α 、 β を生成し保持する。次に、

$$a = \alpha \cdot \beta$$

を計算する。 a は公開情報である。次に、公開情報として、一つ以上の素数を生成し、それから整数 p を作成し、保持する。次に、公開の関数である、 $f(\cdot)$ の形式を定める。次に、Fiat-Shamir 方式のパラメータである、 t と k の値を定める。(ステップ 1 は、一度行えば、ステップ 2 ～ステップ 4 の異なる通信装置への処理に対しても共通である。)

ステップ 2：

任意の通信装置 w についての公開識別情報を、ID_w とする。管理用装置は、通信装置 w からの依頼により、 $j = 1, 2, \dots, k$ について、

と分解する。T を公開のデータとする。E (Z₁, U) を、任意のデータ U を暗号装置により、鍵 Z₁ を用いて暗号化した値とする。この暗号装置には、任意の暗号アルゴリズム（例えば、前述した、FEAL-8 暗号、DES 暗号、RSA 暗号など）を使用可能である。すると、

$$F_1 = E(\theta_1, T) \oplus T$$

$$F_2 = E(\theta_2, F_1) \oplus F_1$$

...

$$F_n = E(\theta_n, F_{n-1}) \oplus F_{n-1}$$

とし、

$$f(\theta) = F_1 \parallel F_2 \parallel \dots \parallel F_n$$

とすることができる。以下では、共通鍵配送の実施例を四つ述べる。

【共通鍵配送の実施例 1】

二重暗号の基本処理手順による共通鍵配送に、Fiat-Shamir 方式によるディジタル署名を適用して、通信装置で相互に相手側の正当性の認証を行う場合について示す。ベキ乗暗号装置は、第 2 図の型のベキ乗暗号装置を用いる。

$$V_{w,j} = f(ID_w, j)$$

を計算する。ここで、 $V_{w,j}$ は、 n を法とする平方剰余であるように、 $j = 1, 2, \dots, k$ を選択する。次に、 $j = 1, 2, \dots, k$ について、管理用装置と、通信装置 w の秘密情報である、

$$S_{w,j} = (1/V_{w,j})^{1/2} \bmod n$$

を求める。ここで、 $S_{w,j}$ は、 $1/V_{w,j}$ の法を n とする最小平方根とする。

ステップ 3：

管理用装置は、通信装置 w に、秘密情報として、 $S_{w,j}$ ($j = 1, 2, \dots, k$) を与える。公開情報である、 n と p の値、および $f(\cdot)$ の形式も与える。 p が合成数のときは、その素因数も与える。Fiat-Shamir 方式のパラメータである、 t と k の値も与える。

ステップ 4：

管理用装置は、通信装置 w に与えるために生成した $V_{w,j}$ と $S_{w,j}$ ($j = 1, 2, \dots, k$) の値を、管理用装置から消去する。

次に、第 1 の過程により、管理用装置から、公

特開平2-301241(5)

開情報、および秘密情報を得た通信装置は、任意の時点で共通鍵配達の第2の過程により、共通鍵の配達を行う。

第4図は、共通鍵配達の第2の過程における電文の交換例である。

共通鍵配達の第2の過程では、通信装置aが共通鍵配達を開始する場合を述べる。(通信装置bが共通鍵配達を開始する場合も同様である)。

共通鍵配達の第2の過程:

ステップ1:

通信装置aは、通信装置aと通信装置bの共通鍵KC_{ab}を生成する。次に、二重暗号の暗号化鍵K₁を乱数により生成する。次に、復号化鍵K₁を、

$$K_{1a} = 1 / K_1 \bmod \phi(p)$$

により求める。次に、

$$AS1 = \exp(KC_{ab} \parallel ID_a, K_1) \bmod p$$

を計算する。次に、乱数R_{1ai} (i=1, 2, ..., t)を生成し、

$$X_{ai} = (R_{1ai})^s \bmod n, (i=1, 2, \dots, t)$$

イジタル署名である。

ステップ2:

通信装置bは、A1を含む電文1を受信する。次に、j=1, 2, ..., kについて、

$$V_{aj} = f(ID_a \parallel j)$$

を計算する。次に、i=1, 2, ..., tについて、

$$Z_{ai} = (Y_{ai})^s \bmod n, G_{aij} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_a = f(AS1 \parallel Z_{ai} \parallel Z_{ai} \parallel \dots \parallel Z_{ai})$$

の先頭k-tビット

が成立することにより、通信装置aのイジタル署名の正当性を検証する。成立しないときは異常終了する。

次に、二重暗号の暗号化鍵K₁を乱数により生成する。次に、復号化鍵K₁を、

$$K_{1b} = 1 / K_1 \bmod \phi(p)$$

により、求める。次に、

$$AS2 = \exp(AS1, K_1) \bmod p$$

$$= \exp(KC_{ab} \parallel ID_a, K_1 \parallel K_1) \bmod p$$

を求める。次に、f(AS1 || X₁ || X₂ || ... || X_t)の先頭k-tビット、を求める。そのk-tビットの個々のビットを、

$$G_{ai} = \{G_{aij}, (i=1, 2, \dots, t; j=1, 2, \dots, k)\}$$

の個々のビットとする。即ち、G_{aij}の要素は、

$$\{G_{ai1}, G_{ai2}, \dots, G_{ai3}, G_{ai4}, G_{ai5}, \dots, G_{ai6}\}$$

である。次に、i=1, 2, ..., tについて、

$$Y_{ai} = R_{ai} \cdot (\prod S_{aij}) \bmod n$$

$$G_{aij} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。ここで、

$$\prod S_{aij} = 1, \text{ for } j=1, 2, \dots, k$$

は、j=1, 2, ..., kについて、G_{aij}=1であるS_{aij}の数を表す。次に、

$$Y_a = Y_{a1} \parallel Y_{a2} \parallel \dots \parallel Y_{at}$$

とする。次に、

$$A1 = \{ID_a, AS1, G_a, Y_a\}$$

を求める。A1を含む電文1を通信装置bに送信する。ここで、G_a、Y_aが電文AS1に対するデ

を計算する。次に、乱数R_{2ai} (i=1, 2, ..., t)を生成し、

$$X_{ai} = (R_{2ai})^s \bmod n, (i=1, 2, \dots, t)$$

を計算する。次に、f(AS2 || X₁ || X₂ || ... || X_t)の先頭k-tビット、を求める。そのk-tビットの個々のビットを、

$$G_b = \{G_{bij}, (i=1, 2, \dots, t; j=1, 2, \dots, k)\}$$

の個々のビットとする。即ち、G_{bij}の要素は、

$$\{G_{b11}, G_{b12}, \dots, G_{b13}, G_{b14}, G_{b15}, \dots, G_{b16}\}$$

である。次に、i=1, 2, ..., tについて、

$$Y_{bi} = R_{bi} \cdot (\prod S_{bij}) \bmod n$$

$$G_{bij} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$Y_b = Y_{b1} \parallel Y_{b2} \parallel \dots \parallel Y_{bt}$$

を作成する。次に、

$$A2 = \{ID_b, AS2, G_b, Y_b\}$$

を作成し、A2を含む電文2を通信装置aに送信する。ここで、G_b、Y_bが、電文AS2に対する通信装置bのイジタル署名である。

ステップ 3:

通信装置 a は、 A_2 を含む電文 2 を受信する。

次に、

$$V_{s,j} = f(I.D., \parallel j), \quad j=1, 2, \dots, k$$

を計算する。次に、 $j=1, 2, \dots, k$ について、

$$Z_{s,j} = (Y_{s,j})^n \prod_{i=1}^k V_{s,i} \bmod p$$

を計算する。次に、

$$G_s = f(A.S.2 \parallel Z_{s,1} \parallel Z_{s,2} \parallel \dots \parallel Z_{s,k})$$

の先頭 $k-t$ ビット

が成立することにより、通信装置 s のディジタル署名の正当性を検証する。成立しないときは異常終了する。次に、

$$A_3 = \exp(A.S.2, K_{1,s}) \bmod p$$

$$= \exp(K_{C,s} \parallel I.D., K_s) \bmod p$$

を計算し、 A_3 を含む電文 3 を通信装置 b に送信する。

ステップ 4:

通信装置 b は、 A_3 を含む電文 3 を受信する。

次に、

$$n = \alpha \cdot \beta$$

を計算する。 n は公開情報である。次に、公開情報として、素数 α を生成し、保持する。次に、公開の関数である、 $f(\cdot)$ の形式を定める。次に、 $ElGamal$ 方式のパラメータである、 i と β の値を定める。

(ステップ1は、一度行えば、ステップ2～ステップ4の異なる通信装置への処理に対しても共通である。)

ステップ 2:

任意の通信装置 w についての公開鍵剥落情報を、 $I.D.$ とする。管理用装置は、通信装置 w からの依頼により、 $j=1, 2, \dots, k$ について、

$$V_{w,j} = f(I.D., \parallel j)$$

を計算する。ここで、 V_j は、 n を法とする平方剰余であるように、 $j=1, 2, \dots, k$ を選択する。次に、 $j=1, 2, \dots, k$ について、管理用装置と、通信装置 w の秘密情報である。

$$S_{w,j} = (1/V_{w,j})^{1/2} \bmod n$$

を求める。ここで、 $S_{w,j}$ は、 $1/V_{w,j}$ の法を n と

$$A_4 = \exp(A_3, K_{1,s}) \bmod p$$

$$= K_{C,s} \parallel I.D.$$

を得る。次に $I.D.$ が正しいかどうかを確認し、正しいときは、共通鍵 $K_{C,s}$ を保持する。 $I.D.$ が正しくないときは異常終了する。

以上の共通鍵配達の過程において、異常が発生時は、その過程は異常終了する。

【共通鍵配達の実施例 2】

$Diffie-Hellman$ による共通鍵配達の方式に、 $ElGamal$ 方式によるディジタル署名を適用して、通信装置で相互に相手側の正当性の認証を行う場合について示す。ベキ乗暗号装置は、第3回のベキ乗暗号装置を用いる。

まず、管理用装置は、各通信装置が管理用装置に登録を行うときに、次の共通鍵配達の第1の過程を実行する。

共通鍵配達の第1の過程:

ステップ 1:

管理用装置は、管理用装置の秘密情報として、素数 α 、 β を生成し保持する。次に、

する最小平方根とする。

ステップ 2:

管理用装置は、通信装置 w に、秘密情報として、 $S_{w,j}$ ($j=1, 2, \dots, k$) を与える。また公開情報である、 n 、 $f(\cdot)$ 、 H も与える。 $ElGamal$ 方式のパラメータである、 i と β の値も与える。

ステップ 3:

管理用装置は、通信装置 w に与えるために生成した $V_{w,j}$ と $S_{w,j}$ ($j=1, 2, \dots, k$) の値を、管理用装置から消去する。

次に、第1の過程により、管理用装置から、公開情報、および秘密情報を得た通信装置は、任意の時点で共通鍵配達の第2の過程により、共通鍵の配達を行う。

第5回は、共通鍵配達の第2の過程における電文の交信例である。

共通鍵配達の第2の過程では、通信装置 a が鍵配達を開始する場合を述べる。(通信装置 b が鍵配達を開始する場合も同様である)。

共通鍵配達の第2の過程:

ステップ1:

通信装置aは、秘密情報T_aを乱数により生成する。次に、

$$W_a = \exp(H, T_a) \bmod p$$

を求める。次に、乱数R_{aij} (i=1, 2, ..., l, j=1, 2, ..., l)を生成し、

$$X_{aij} = (R_{aij})^2 \bmod n, (i=1, 2, \dots, l)$$

を求める。次に、f (W_a || X₁₁ || X₁₂ || ... || X_{1l})の先頭k・tビット、を求めて、そのk・tビットの個々のビットを、

$$G_{aij} = \{G_{aij}, (i=1, 2, \dots, l; j=1, 2, \dots, l)\}$$

の個々のビットとする。次に、i=1, 2, ..., lについて、

$$Y_{aij} = R_{aij} \cdot (\prod S_{aj}) \bmod n$$

$$G_{ajj} = 1, \text{ for } j=1, 2, \dots, l$$

を計算する。次に、

$$Y_a = Y_{a1} || Y_{a2} || \dots || Y_{al}$$

とする。次に、

$$KC_{aa} = \exp((\exp(W_a, T_a) \bmod p), T_a) \bmod p$$

$$= \exp(E, T_a, T_a) \bmod p$$

を計算する。次に、共通鍵KC_{aa}を、

$$KC_{aa} = KC_{Qaa} \text{の先頭からの部分ビット (ビット長L)}$$

により求め保持する。ビット長Lは、共通鍵のビット長である。次に、

$$W_b = \exp(H, T_b) \bmod p$$

を計算する。次に、乱数R_{bij} (i=1, 2, ..., l, j=1, l)を生成し、

$$X_{bij} = (R_{bij})^2 \bmod n, (i=1, 2, \dots, l)$$

を求める。次にf (W_b || X₁₁ || X₁₂ || ... || X_{1l})の先頭k・tビット、を求めて、そのk・tビットの個々のビットを、

$$G_{bij} = \{G_{bij}, (i=1, 2, \dots, l; j=1, 2, \dots, l)\}$$

の個々のビットとする。次に、i=1, 2, ..., lについて、

$$Y_{bij} = R_{bij} \cdot (\prod S_{bj}) \bmod n$$

$$G_{bjj} = 1, \text{ for } j=1, 2, \dots, l$$

$$B_1 = \{ID_a, W_a, G_a, Y_a\}$$

を求めて、B₁を含む電文1を通信装置bに送信する。ここで、G_a, Y_aが共通鍵の配達に関する電文W_aに対するデジタル署名である。

ステップ2:

通信装置bは、B₁を含む電文1を受信する。次に、通信装置bは、秘密情報T_bを乱数により生成する。次に、

$$V_{bij} = f(ID_b, || j), j=1, 2, \dots, k$$

を計算する。次に、i=1, 2, ..., lについて、

$$Z_{bij} = (Y_{bij})^2 \bmod n$$

$$G_{bij} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_b = f(W_b || Z_{b1} || Z_{b2} || \dots || Z_{bl})$$

$$\text{の先頭k・tビット}$$

が成立することにより、通信装置aのデジタル署名の正当性を検証し、成立しないときは異常終了する。次に、通信装置bは秘密情報T_bを乱数により生成し、

を計算する。次に、

$$Y_b = Y_{b1} || Y_{b2} || \dots || Y_{bl}$$

とする。次に、

$$B_2 = \{ID_b, W_b, G_b, Y_b\}$$

とする。次に、B₂を含む電文2を通信装置aに送信する。ここで、G_b, Y_bが、共通鍵配達に関する電文W_bに対する通信装置bのデジタル署名である。

ステップ3:

通信装置aは、B₂を含む電文2を受信する。次に、

$$V_{bij} = f(ID_a, || j), j=1, 2, \dots, k$$

を計算する。次に、i=1, 2, ..., lについて、

$$Z_{bij} = (Y_{bij})^2 \bmod n$$

$$G_{bij} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_b = f(W_b || Z_{b1} || Z_{b2} || \dots || Z_{bl})$$

$$\text{の先頭k・tビット}$$

が成立することにより、通信装置bのデジタル

署名の正当性を検証する。成立しないときは異常終了する。次に、

$$KC_{11} = \exp((\exp(B, T_1) \bmod p), T_2) \bmod p \\ = \exp(B, T_1 \cdot T_2) \bmod p$$

を計算し、

$$KC_{11} = KCQ_{11} \text{ の先頭からの部分ビット (ビット長 L)}$$

とし、 KC_{11} を保持する。

なお、以上の共通鍵配送の過程において、異常が発生時は、その過程は異常終了する。

[共通鍵配送の実施例 3]

RSA暗号による鍵配送に、Fiat-Shamir方式によるデジタル署名を適用して、通信装置で相互に相手側の正当性の認証と共通鍵の配送を行う場合について示す。ベキ乗暗号装置は、第2図のベキ乗暗号装置を用いる。

まず、管理用装置は、各通信装置が管理用装置に登録を行うときに、次の共通鍵配送の第1の過程を実行する。

共通鍵配送の第1の過程：

$$S_{ws} = (1/V_{ws})^{1/2} \bmod n$$

を求める。ここで、 S_{ws} は、 $1/V_{ws}$ の法を n とする最小平方根とする。

ステップ 3：

管理用装置は、通信装置 w に、秘密情報として、 S_{ws} 、 $(j = 1, 2, \dots, k)$ を与える。また、公開情報である、 n $f(\cdot)$ も与える。Fiat-Shamir方式のパラメータである、 t との値も与える。

ステップ 4：

管理用装置は、通信装置 w に与えるために生成した V_{ws} 、 S_{ws} 、 $(j = 1, 2, \dots, k)$ の値を、管理用装置から消去する。

次に、第1の過程により、管理用装置から、公開情報、および秘密情報を得た通信装置は、任意の時点で共通鍵配送の第2の過程により、共通鍵の配送を行う。

第6図は、共通鍵配送の第2の過程における電文の交換例である。

共通鍵配送の第2の過程では、通信装置 a が鍵

ステップ 1：

管理用装置は、管理用装置の秘密情報として、素数 α 、 β を生成し保持する。次に、

$$n = \alpha \cdot \beta$$

を計算する。 n は公開情報である。次に、公開の因数である、 $f(\cdot)$ の形式を定める。次に、Fiat-Shamir方式のパラメータである、 t と k の値を定める。

(ステップ1は、一度行えば、ステップ2～ステップ4の異なる通信装置への処理に対しても共通である。)

ステップ 2：

任意の通信装置 w についての公開識別情報を、 ID_w とする。管理用装置は、通信装置 w からの依頼により、 $j = 1, 2, \dots, k$ について、

$$V_j = f(ID_w \parallel j)$$

を計算する。ここで、 V_{ws} は、 n を法とする平方剰余であるように、 $j = 1, 2, \dots, k$ を選択する。次に、 $j = 1, 2, \dots, k$ について、管理用装置と、通信装置 w の秘密情報である、

配送を開始する場合を述べる。(通信装置 b が鍵配送を開始する場合も同様である。)

共通鍵配送の第2の過程：

ステップ 0：

通信装置 a は、RSA暗号の公開鍵(暗号化部) PK_a 、秘密の素数 P_a, Q_a 、公開の整数 N_a 、および秘密鍵(復号化部) SK_a を生成する。

$$N_a = P_a \cdot Q_a$$

であり、 P_a と Q_a は通信装置 a の秘密の素数である。また、

$$PK_a \cdot SK_a \equiv 1 \pmod{N_a}$$

である。通信装置 a は、 $PK_a, N_a, SK_a, P_a, Q_a$ を保持する。

(ステップ0は、一度行っておけば、以後に共通鍵配送の第2の過程を再び行うときは、省略できる。)

ステップ 1：

通信装置 a は、乱数 R_{ai} 、 $(i = 1, 2, \dots, t)$ を生成し、

$$X_{ai} = (R_{ai})^2 \bmod n, (i = 1, 2, \dots, t)$$

特開平2-301241(9)

を計算する。次に、 $I(PK, \|N, \|X_{11}\| \dots \|X_{1k}\|)$ の先頭 $k \cdot t$ ビット、を求める、その $k \cdot t$ ビットの個々のビットを、

$$G_{1i} = (G_{11i}, (i=1, 2, \dots, t; j=1, 2, \dots, k))$$

の個々のビットとする。次に、 $i=1, 2, \dots, t$ について、

$$Y_{1i} = R_{1i} \cdot (\prod S_{1ij} \bmod n \\ G_{11j} = 1, \text{ for } j=1, 2, \dots, k)$$

を求める。次に、

$$Y_1 = Y_{11} \| Y_{12} \| \dots \| Y_{1k}$$

とする。次に、

$$C_1 = (ID_a, PK_a, N_a, G_a, Y_1)$$

とする。次に C_1 を含む電文 1 を通信装置 b に送信する。ここで、 G_a, Y_1 が電文 PK_a に対する通信装置 a のデジタル署名である。

ステップ 2:

通信装置 b は、 C_1 を含む電文 1 を受信する。
次に、通信装置 b は、

$$V_{21} = I(ID_b, \|1), j=1, 2, \dots, k$$

$$Y_{21} = R_{21} \cdot (\prod S_{21j} \bmod n \\ G_{21j} = 1, \text{ for } j=1, 2, \dots, k)$$

を計算する。次に、

$$C_2 = (ID_b, W_1, G_a, Y_1)$$

を求め、 C_2 を含む電文 2 を、通信装置 a に送信する。ここで、 G_a, Y_1 が、電文 W_1 に対する通信装置 b のデジタル署名である。

ステップ 3:

通信装置 a は、 C_2 を含む電文 2 を受信する。
次に、

$$V_{2j} = I(ID_b, \|1), j=1, 2, \dots, k$$

を計算する。次に、 $i=1, 2, \dots, t$ について、

$$Z_{2i} = (Y_{2i})^k \prod V_{2ij} \bmod n \\ G_{21j} = 1, \text{ for } j=1, 2, \dots, k$$

を計算する。次に、

$$G_b = I(W_1 \| Z_{21} \| Z_{22} \| \dots \| Z_{2k})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置 b のデジタル署名の正当性を検証する。成立しないときは異常終了する。次に、

を計算し、 $i=1, 2, \dots, t$ について、

$$Z_{3i} = (Y_{3i})^k \prod V_{3ij} \bmod n \\ G_{31j} = 1, \text{ for } j=1, 2, \dots, k$$

を求める。次に、

$$G_a = I(PK_a, \|N_a, \|Z_{21} \| Z_{22} \| \dots \| Z_{2k})$$

が成立することにより、通信装置 a のデジタル署名を検証し、成立しないときは、異常終了する。次に、共通鍵 KC_{ab} を生成し、

$$W_1 = \exp (KC_{ab}, PK_a) \bmod N_a$$

を求める。次に、乱数 $R_{31j}, (i=1, 2, \dots, t)$ 、を生成し、

$$X_{3i} = (R_{31j})^k \bmod n$$

を求める。次に $I(ID_a, \|X_{31} \| X_{32} \| \dots \| X_{3k})$ の先頭 $k \cdot t$ ビット、を求める、その $k \cdot t$ ビットの個々のビットを、

$$G_b = (G_{31j}, (i=1, 2, \dots, t; j=1, 2, \dots, k))$$

の個々のビットとする。次に、 $i=1, 2, \dots, t$ について、

$$Z_{22} = \exp (W_1, SK_a) \bmod N_a \\ = \exp (KC_{ab}, PK_a, SK_a) \bmod N_a \\ = KC_{ab}$$

を求める、これにより共通鍵 KC_{ab} を得て保持する。

なお、以上の共通鍵配達の過程において、異常が発生時は、その過程は異常終了する。

【共通鍵配達の実施例 4】

二重暗号の基本処理手順による共通鍵配達に、Flat-Shamir 方式によるデジタル署名を適用して、通信装置で相互に相手側の正当性の認証を行う場合について、実施例 1 とは別の実施例を示す。デジタル署名を実施例 1 とは別の電文に適用する例である。ベキ乗暗号装置は、第 2 図の型のベキ乗暗号装置を用いる。

まず、管理用装置は、各通信装置が管理用装置に登録を行うときに、次の共通鍵配達の第 1 の過程を実行する。

共通鍵配達の第 1 の過程：

共通鍵配達の実施例 1 の、共通鍵配達の第 1 の過程と同じである。

共通鍵配送の第2の過程:

ステップ1:

通信装置aは、通信装置aと通信装置bの共通鍵 $K_{C_{ab}}$ を生成する。次に、二重暗号の暗号化鍵 K_1 を乱数により生成する。更に、復号化鍵 K_{1a} を、

$$K_{1a} = 1 / K_1 \bmod \phi(p)$$

により求められる。次に、

$$A_1 = \exp(K_{C_{ab}} \parallel ID_a, K_1) \bmod p$$

を計算し、 A_1 を含む電文1を通信装置bに送信する。

ステップ2:

通信装置bは、 A_1 を含む電文1を受信する。次に、二重暗号の暗号化鍵 K_1 を乱数により生成する。次に、復号化鍵 K_{1b} を、

$$K_{1b} = 1 / K_1 \bmod \phi(p)$$

により求める。次に、

$$AS_2 = \exp(A_1, K_1) \bmod p$$

$$= \exp(K_{C_{ab}} \parallel ID_a, K_1 \parallel K_1) \bmod p$$

を計算する。次に、乱数 $R_{ab,i}$ ($i = 1, 2, \dots, t$)

次に、

$$V_{ab,j} = f(ID_b \parallel j), j = 1, 2, \dots, k$$

を計算する。次に、 $i = 1, 2, \dots, t$ について、

$$Z_{ab,i} = (Y_{ab,i})^k \parallel V_{ab,i} \bmod n$$

$$G_{ab,i} = 1, \text{ for } j = 1, 2, \dots, k$$

を計算する。次に、

$$G_a = f(AS_2 \parallel Z_{ab,1} \parallel Z_{ab,2} \parallel \dots \parallel Z_{ab,t})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置bのデジタル署名の正当性を検証する。成立しないときは異常終了する。次に、

$$AS_3 = \exp(AS_2, K_{1a}) \bmod p$$

$$= \exp(K_{C_{ab}} \parallel ID_a, K_1 \parallel K_1) \bmod p$$

を計算する。次に、乱数 R_a を生成し、

$$X_{ab,i} = (R_{ab,i})^k \bmod n, (i = 1, 2, \dots, t)$$

を求める。次に、

$$G_a = f(AS_3 \parallel X_{ab,1} \parallel X_{ab,2} \parallel \dots \parallel X_{ab,t})$$

の先頭 $k \cdot t$ ビット

を求める。次に、 $i = 1, 2, \dots, t$ について

\dots, i を生成し、

$$X_{ab,i} = (R_{ab,i})^k \bmod n, (i = 1, 2, \dots, t)$$

を計算する。次に、 $f(AS_2 \parallel X_{ab,1} \parallel X_{ab,2} \parallel \dots \parallel X_{ab,t})$ の先頭 $k \cdot t$ ビットを求める。更に、 $k \cdot t$ ビットの個々のビットを、

$$G_a = \{G_{ab,i,j}, (i = 1, 2, \dots, t; j = 1, 2, \dots, k)\}$$

の個々のビットとする。次に、 $i = 1, 2, \dots, t$ について、

$$Y_{ab,i} = R_{ab,i} \cdot (\prod S_{ab,j}) \bmod n$$

$$G_{ab,i} = 1, \text{ for } j = 1, 2, \dots, k$$

を計算する。次に、

$$Y_a = Y_{ab,1} \parallel Y_{ab,2} \parallel \dots \parallel Y_{ab,t}$$

とする。次に、

$$A_2 = \{ID_a, AS_2, G_a, Y_a\}$$

とする。次に、 A_2 を含む電文2を通信装置aに送信する。ここで、 G_a, Y_a が電文AS2に対する通信装置bのデジタル署名である。

ステップ3:

通信装置aは、 A_2 を含む電文2を受信する。

て、

$$Y_{ab,i} = R_{ab,i} \cdot (\prod S_{ab,j}) \bmod n$$

$$G_{ab,i} = 1 \text{ for } j = 1, 2, \dots, k$$

を計算する。 $Y_a = Y_{ab,1} \parallel Y_{ab,2} \parallel \dots \parallel Y_{ab,t}$ とする。ここで、 G_a, Y_a が電文AS3に対する通信装置aのデジタル署名である。次に、

$$A_3 = \{ID_a, AS_3, G_a, Y_a\}$$

を計算し A_3 を含む電文3を通信装置bに送信する。

ステップ4:

通信装置bは、 A_3 を含む電文3を受信する。

次に、

$$V_{ab,j} = f(ID_b \parallel j), j = 1, 2, \dots, k$$

を計算する。次に、 $i = 1, 2, \dots, t$ について、

$$Z_{ab,i} = (Y_{ab,i})^k \parallel V_{ab,i} \bmod n$$

$$G_{ab,i} = 1, \text{ for } j = 1, 2, \dots, k$$

を計算する。次に、

$$G_a = f(AS_3 \parallel Z_{ab,1} \parallel Z_{ab,2} \parallel \dots \parallel Z_{ab,t})$$

の先頭 $k \cdot t$ ビット

が成立することにより、通信装置aのデジタル

署名を検証する。成立しないときは異常終了する。
成立したときは、

$$A_4 = \exp(A_3 \cdot K_{1,}) \bmod p$$

$$= K_{C,} \cdot I \cdot D,$$

を計算し、I · D の正当性を確認し、異常のときは異常終了し、正当なときは、共通鍵 $K_{C,}$ を得て保持する。

以上の共通鍵配達の過程において、異常が発生時は、その過程は異常終了する。なお、この発明では、以下の選択も可能である。

- ① この発明の適用に際して利用する通信網の物理的構成（例えば、専用線、交換回線、機内網など）、通信網インターフェース、及び通信プロトコルは、任意に選択できる。
- ② この発明の実施例では、ベキ乗暗号装置を用いた共通鍵配達に Fiat-Shamir 方式によるディジタル署名を適用する場合を記述したが、Fiat-Shamir 方式と類似の通信形態を有するディジタル署名方式（例えば、Fiat-Shamir 方式の、別のパラメータ選択の利用、拡張、改良）も、

この発明に適用できることは明らかであり、そのような場合もこの発明は含んでいる。

- ③ この発明の共通鍵配達の実施例 3 では、公開鍵暗号に RSA 暗号を用いる場合を述べたが、Rabin 暗号などの、他の公開鍵暗号も用いることが可能であり、この発明は、そのような場合も含んでいる。
- ④ 実施例では、管理用装置が 1 つの場合を述べたが、管理用装置が複数の場合も、各管理用装置の処理は同様である。その場合、管理用装置の秘密情報を公開情報を個別、または共通にすることにより、個々の管理用装置を独立させるとか、または一体とするかを選択できる。

「発明の効果」

この発明の共通鍵配達方式は、次の長所がある。

- ① 管理用装置の情報は、通信装置ではデジタル署名にのみ用いられるので、万一に第三者に透けしても、共通鍵が洩れないので安全性が高い。また、管理用装置は、共通鍵を知ることができないので、通信装置の共通鍵の秘密は保た

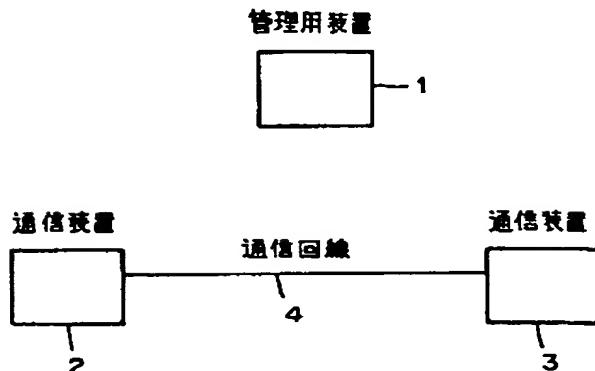
れる。

- ② 通信装置は、共通鍵配達時に、管理用装置との通信が不要であるので、管理用装置と通信不能となつても、通信装置の間では暗号通信が可能である。

4. 図面の簡単な説明

第 1 図は通信システムの一構成例を示すプロック図、第 2 図はベキ乗暗号装置の一構成例を示すプロック図、第 3 図は第 2 図と異なるベキ乗暗号装置の一構成例を示すプロック図、第 4 図は共通鍵配達の実施例 1 の共通鍵配達第 2 の過程における電文の交信例を示す図、第 5 図は共通鍵配達の実施例 2 の共通鍵配達第 2 の過程における電文の交信例を示す図、第 6 図は共通鍵配達の実施例 3 の共通鍵配達第 2 の過程における電文の交信例を示す図である。

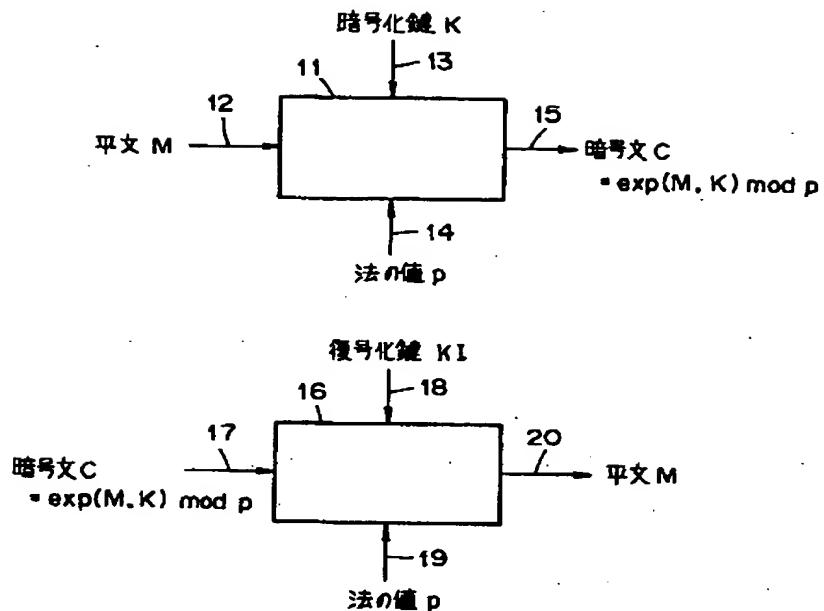
第 1 図



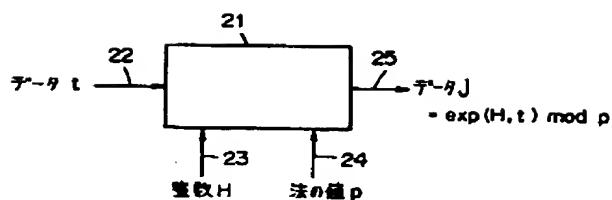
特許出願人 日本電信電話株式会社

代理人 車野卓

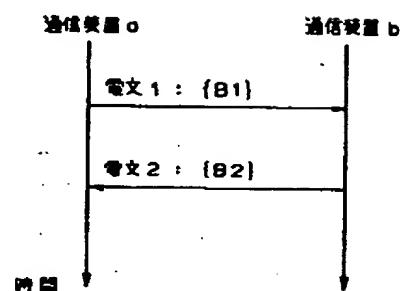
第2図



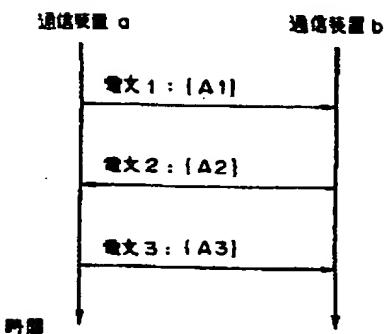
第3図



第5図



第4図



第6図

